Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 10 (2012) 713 – 720

Procedia Computer Science

The 9th International Conference on Mobile Web Information Systems (MobiWIS)

Trust-based Throughput in Cognitive Radio Networks

Sazia Parvin[a,*], Farookh Khadeer Hussain[b], Omar Khadeer Hussain[a], Abdullah Al Faruque[a]

[a]*Curtin Business School, Curtin University, Perth, 6102, Australia*
[b]*School of Software, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW*

Abstract

Cognitive Radio Networks (CRNs) deal with opportunistic spectrum access in order to fully utilize the scarce of spectrum resources, with the development of cognitive radio technologies to greater utilization of the spectrum. Now-a-days Cognitive Radio (CR) is a promising concept for improving the utilization of limited radio spectrum resources for future wireless communications and mobile computing. In this paper, we propose two approaches. At first we propose a trust aware model to authenticate the secondary users (SUs) in CRNs which provides a reliable technique to establish trust for CRNs. Secondly, we propose trust throughput mechanism to measure throughput in CRNs.

Keywords: Trust; spectrum; availability; primary user (PU); secondary user (SU).

1. Introduction

Cognitive Radio (CR) has been considered as a promising concept for improving the utilization of limited radio spectrum resources for future wireless communications and mobile computing.

Cognitive radio pioneered by Mitola [2] from software defined radio (SDR) was originally considered to improve spectrum utilization. The usage of radio spectrum resources and the regulation of radio emissions are coordinated by national regulatory bodies like the Federal Communications Commission (FCC).

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address:sazia.parvin@postgrad.curtin.edu.au

doi:10.1016/j.procs.2012.06.091

Cognitive radio, on the other hand, sits above the SDR (Software Defined Radio) and is the “intelligence” that lets an SDR determine which mode of operation and parameters to use. Actually an SDR is simply a radio that puts most of the Radio Frequency (RF) and Intermediate frequency (IF) functionality, including waveform synthesis, into the digital (rather than the analog) domain, allowing great flexibility in the modes of radio operation (called “personalities”) [2].

The CNRs are composed of various kinds of communication systems and networks, and can be views as a sort of heterogeneous networks. A CR is designed to be aware of and sensitive to the changes in its surroundings, which makes spectrum sensing an important requirement for the realization of CRNs. Spectrum sensing enables CR users to adapt the environment by detecting the spectrum holes without causing interference to the primary user (PU) of network [15]. But if the unlicensed user who is always intended to search free spectrum is not a trustworthy node, then it can break down the normal activities of the CRNs by injecting some malicious attacks. In this paper, firstly we propose a trust aware model which can provide a reliable approach to establish trust for authenticating secondary user (SU) in CRNs for dynamically access the spectrum for transmission in CRNs. Secondly, we propose a stochastic approach to show the free spectrum availability for authenticated SU’s usage in CRNs. The main contribution of this paper is to check the trustworthiness of SUs in CRNs and the free spectrum availability for authenticated SUs in CRNs. The organization of this paper is as follows: In Section 2, related works is reviewed. In Section 3, system architecture of our proposed model is described. In Section 4 and 5, we show how trust is calculated to check the authentication of SUs and the free spectrum availability depending on the stochastic process based on Markov Model respectively. We conclude the paper in Section 6 including future remarks.

2. Related Works

Establishing trust for CRNs is an open and challenging issue for ensuring smooth operation of CRNs to support ubiquitous computing. Trust has been widely mentioned in literatures regarding trusted computing and web computing, ad hoc networks and even social science [7]. However, trust for CRNs is completely different from all of these scenarios. Trust is critical in CRNs operation and beyond security design, as security usually needs communication overhead in advance.

The impact of trust model on CRNs is discussed briefly in [9]. The authors in [10] integrated trust and reputation for the threat mitigation of Spectrum Sensing Data Falsification (SSDF) attack on CRNs. However, they did not propose any trust modeling for CRNs. The authors suggested potential ways for incorporating trust modeling to CRNs including identity management, the trust building process and possible mechanisms for disseminating the trust information [9]. Furthermore, no experimental results were established for these discussions. A trust aware model was proposed for spectrum sensing in CRNs but no numerical result was presented in this paper [14]. A Continuous-time Markov chain model is used to model the spectrum access in CRNs [12]. A non-random channel assignment is proposed in-order to avoid the transition states and to decrease the dropping and blocking probabilities of the SUs [12]. In this paper, we incorporate trust for authenticating SUs in CRNs and propose stochastic approach to find out the free spectrum availability for authenticated SUs in CRNs.

3. System Architecture

A Cognitive Radio Networks (CRNs) is a network composed of Cognitive Radio (CR) nodes that, through learning and reasoning, dynamically adapt to varying network conditions in order to optimize end-to-end performance. As like Wireless Networks, CRNs can be deployed in various kinds of network configurations such as Centralized, Ad-hoc and Mesh Architecture. Figure 1 shows a general architecture of CRNs.

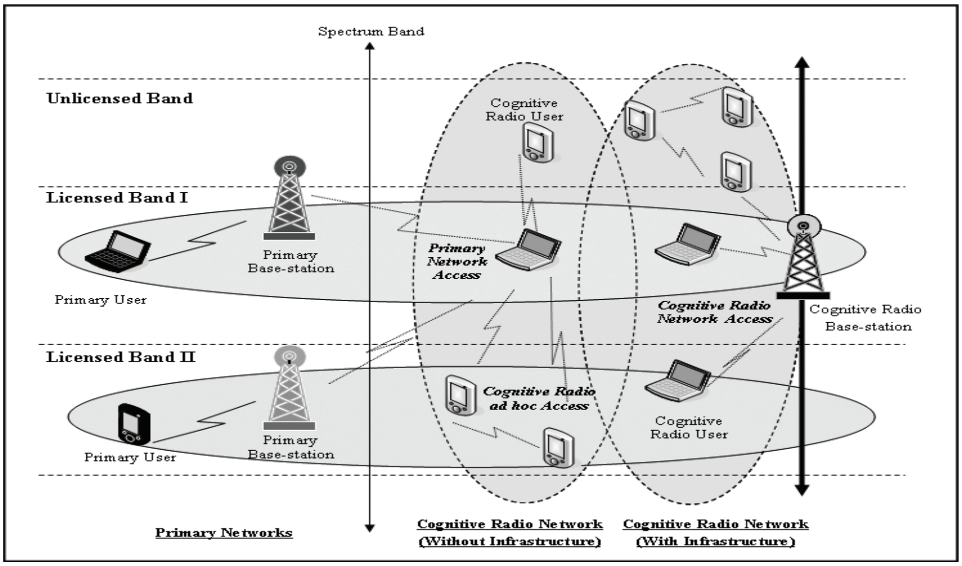

Fig. 1. Cognitive Radio Network Architecture [11]

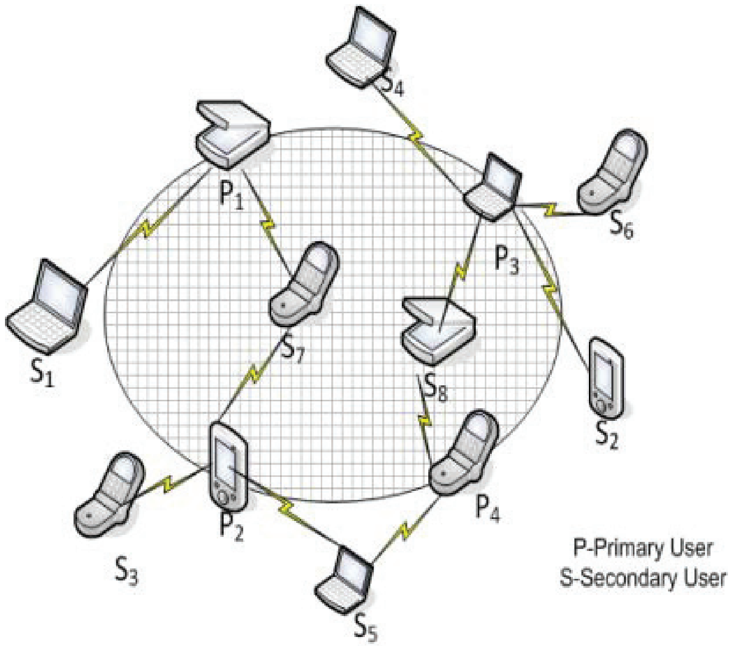

Fig. 2. System Architecture of Proposed Model

In our system architecture, we assume that primary users (PUs) coexist with SUs in some geographical area. In this CRNs architecture, SUs sense the spectrum surrounding and detect the unused spectrum and sharing it without harmful interference with other users as depicted in Figure 2. If SUs can detect more than one PU's free spectrum, Cognitive radios should decide on the best spectrum band to meet the Quality of service requirements over all available spectrum bands. In our system architecture, we depict that SUs will sense a free spectrum hole and to dynamically access the spectrum for transmission. It will achieve "trust" from the PU without creating interference to it. The SU can use the PU's free spectrum as soon as it achieves the trustworthiness. This notion is depicted in Figure 3.

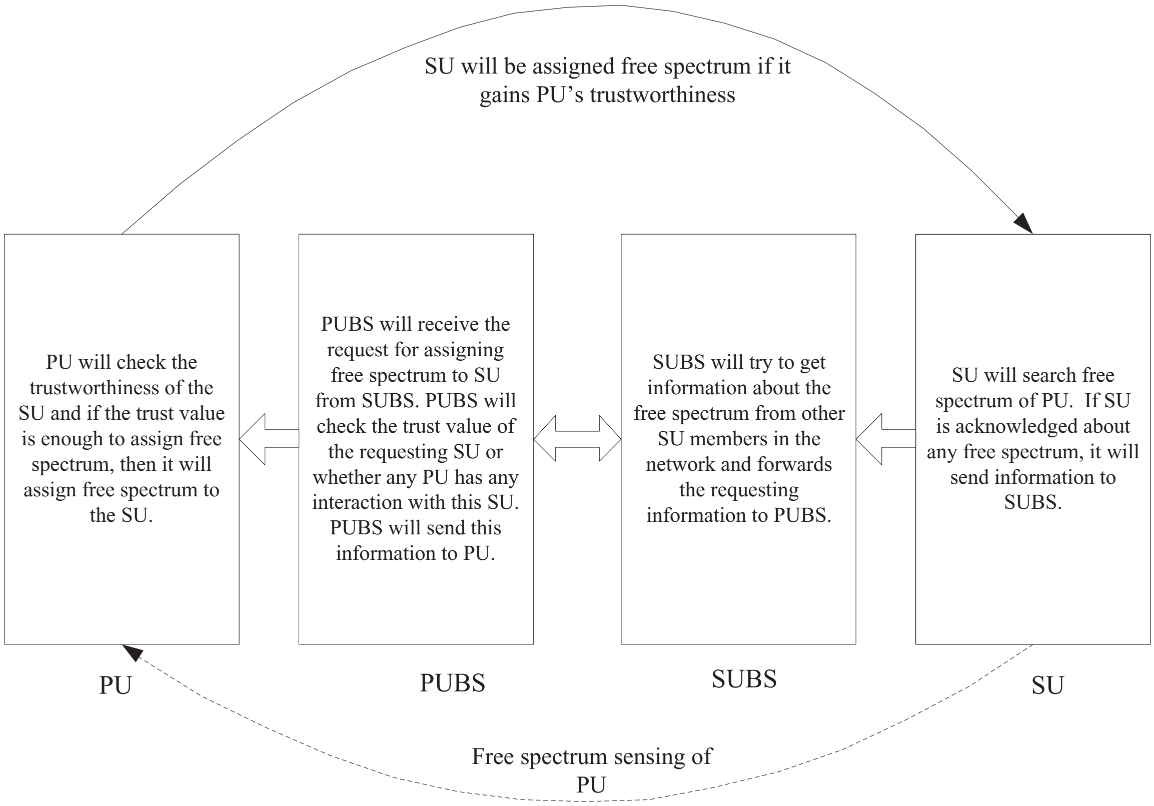

Fig. 3. Interaction between primary user and secondary users in CRNs

4. Trust Model for CRNs

In our new model, we build trust model for cognitive radio networks. Whenever the SU will be assigned free spectrum after checking the trustworthiness depending on trust value, the SU's communication activity will depend on the free spectrum's availability. So in this paper, we propose the stochastic approach based on Markov model to show the spectrum availability for SUs after being an authenticated user in CRNs depending on trust value. The flowchart of our trust model is shown in the Figure 4.

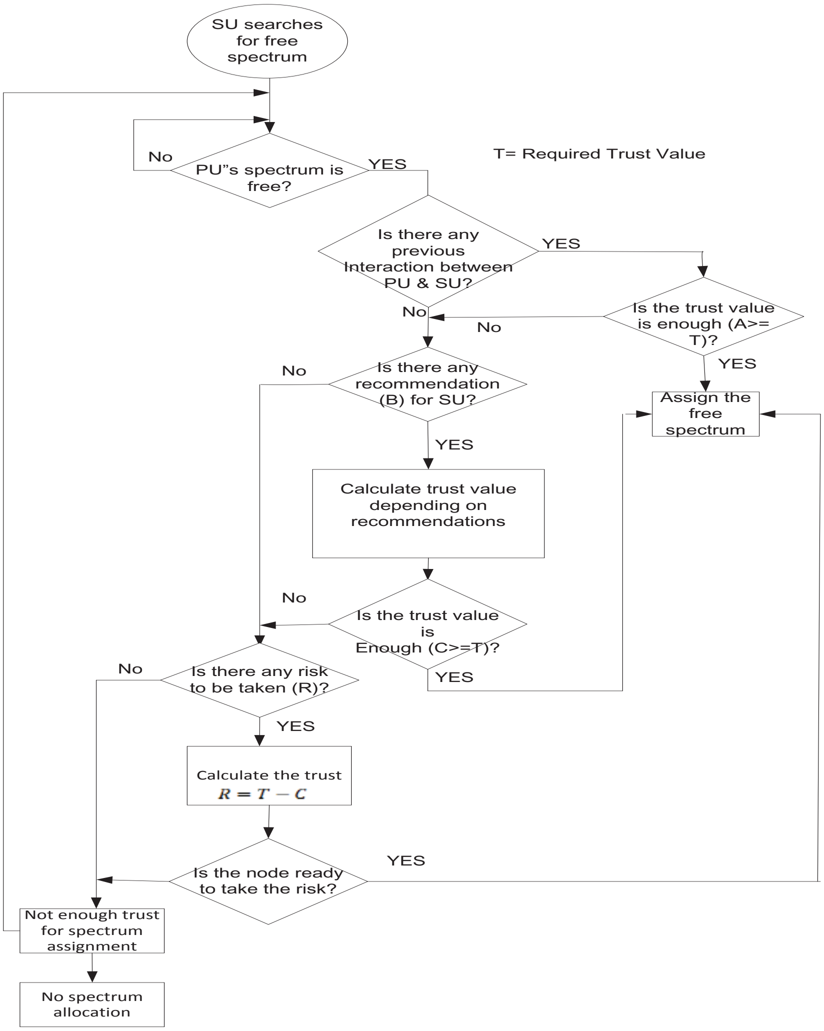

Fig. 4. Flowchart of Trust Model

Each cognitive node will calculate trust for all its surrounding nodes and store these values for later use; these values should be updated in a specific time period based on new interactions.

The illustration of the flowchart given in Figure 4 is as follows. Initially when a secondary node tries to use one of PU's free spectrum band, at first the SU searches PU's free spectrum. If the PU's spectrum band is free, the first thing PU will do is to check the interaction, if it had any previous interaction with this SU. If that's the case, the PU will check if the trust level on this SU is enough to assign free spectrum or not. If the trust value (A) is enough by checking (A>=T?), where T is the required Trust then the PU will assign free spectrum to this SU. If the trust value (A) is not enough, the PU will look for any recommendations (B) about the SU from the surrounding nodes. If there is, the PU will calculate the trust value depending on this recommendations (B) and check again to see if the trust value (C>=T ?) is enough to assign the spectrum. If the trust value (C) is not enough or in case of a new SU (no interactions or recommendations available for this SU), then the PU will check the amount of risk value to continue interaction with the SU. If the PU is ready to take the risk level regarding the association with the SU, then the PU will assign the free spectrum to the SU. Otherwise the whole process will be declined and the SU will try to search other PU's spectrum band.

From the above description and by referring to the flowchart algorithm, the trust value of PU to SU can be any of the following values (A, B, C, R).

$$T_{PU}(SU) = \begin{cases} A, \text{if the trust from previous interation is enough} \\ B, \text{if the trust from recommendation is enough} \\ C, \text{if } f(A,B) \text{ value is enough} \\ R, \text{if there is any risk} \end{cases}$$

Each of these values can be calculated as follows:

$$A = \sum_{i=1}^{i=n} T_{PU}(i) \qquad (1)$$

Where, $T_{PU}(i)$-trust value of the ith trust category,
n- number of trust categories.

$$B = \frac{\sum_{j=1}^{n} T_j(Su)}{n} \qquad (2)$$

Where, $T_j(x)$-trust value of node j on SU node,
n-number of the surrounding nodes.
And Risk value can be calculated as:

$$Risk\ Value\ \ R = T - C \qquad (3)$$

Where T is required trust Value
And $C = f_1\ (A, B)$ (4)
In equation 4, the 'C ' value will be calculated by integrating of A and B. This process is called data fusion method.

After the PU performs these trust calculations, the SU will be authenticated to the CRNs depending on the trust value. Whenever the SU will be trustworthy to the PU, then SU will be able to use PU's free spectrum band. In the next section we show the spectrum availability of SU depending on the stochastic process which is based on Markov Model.

5. Trust Throughput for Cognitive Radio Nodes

Depending on the trustworthy relation between Primary users and Secondary users, we measure the trust throughput depending on the trust model depicted in Figure 5. In this model, PU1 has trust on SU1 depending on T11 trust value. SU1 also trusts SU3 depending on T12 trust value. So the trust value (t13) between PU1 and SU3 called `` Maximum Trust Throughput'' and can be calculated by the equation (5). Here we are assuming two types of trust. One is `direct trust' which exists between one hop neighbours of primary users and secondary users called `Medium trust'. Another is one is `indirect trust' which exists between all Secondary Users and is called `Second Medium Trust'.
The trust value between PU1 and SU3 (T13) is:
t13=min {T11, T12}
We assume the trust value for Medium Trust, Second Medium Trust and Maximum Trust Throughput in the following table:

Table 1. Trust table

Trusted Nodes	Trust Symbols	Trust Value
PU1, SU1	T11	.1
SU1, SU3	T12	.2
PU1, SU3	t13	.2
PU2, SU3	T23	.2
SU3, SU1	T31	.3
PU2, SU1	t21	.2
PU4, SU3	T43	.3
SU3, SU2	T32	.4
PU4, SU2	t42	.1
PU2, SU2	t22	.2
PU4, SU1	t41	.1
PU3,SU3	T33	.4
SU3,SU4	T34	.5
PU3,SU4	t34	.3

If we categorize the trust value according to above trust Table 1, we can get the following category of trust value:

Medium Trust: which is Direct Trust from Primary User to Secondary User ; Second Medium Trust : which from Secondary Users to Secondary Users; Maximum Trust Throughput : which is Indirect trust from Primary Users to Secondary Users; Medium Trust Value is: {.1, .2,.3,.4 }; Second Medium Trust Value is: ={.2,.3,.4,.5 }; Maximum Trust Throughput is: {.1,.2,.3,.4}.

Figure 6 shows the relation between Medium trust, second medium trust and maximum trust throughput.

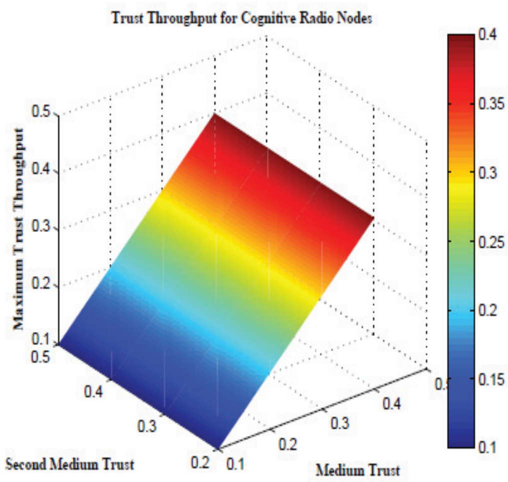

Fig. 6. Trust Throughput of nodes in CRNs;

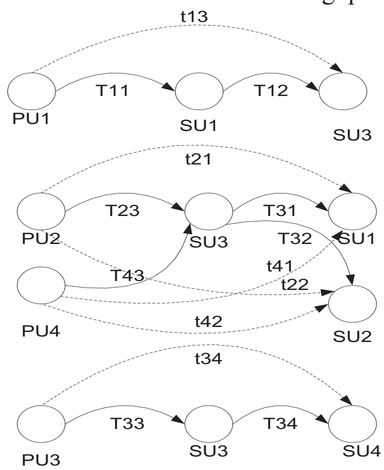

Fig. 5. Trust Throughput

In Figure 6, we show that if the medium trust and second medium trust is increased then maximum trust throughput is increased. There is closely proportional relation between these three trust categories.

6. Conclusion

In cognitive radio networks, some cruel secondary users may create interference by accessing the primary user's available spectrum band. Such malicious SUs can seriously break down the whole network performance. To tackle this problem, we want to use a trust aware model to check the trustworthiness of the secondary user who wants to use primary user's free spectrum band. After checking the authentication, the system can allocate free spectrum to secondary users in cognitive radio networks. In order to realize the ideas, we have proposed a trust aware spectrum sensing model for secondary users to be authenticated in cognitive radio networks. Secondly we have proposed a trust throughput mechanism to ensure data transmission between primary and secondary users in CRNs.

References

[1] Mohammad, M. et al. A New Algorithm of Trust Formation in Wireless Sensor Networks. in AusWireless'06. 2006. Sydney, Australia.

[2] Mitola, J. Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. PhD thesis, in Royal Institute of Technology (KTH). 2000.

[3] Haykin, S. Cognitive radio: brain-empowered wireless communications IEEE Journal on Selected Areas in Communications, 2005. 23(2): p. 201-220.

[4] Chen, K.-C. et al. Cognitive radio network architecture: part I -- general structure. in Proceedings of the 2nd international conference on Ubiquitous information management and communication 2008. Suwon, Korea ACM.

[5] FCC, E T Docket No 03-222 Notice of Proposed rule making and order. December, 2003..

[6] Han, G., Choi, D., Lim, W. A Reliable Approach of Establishing Trust for Wireless Sensor Networks. in IFIP International Conference, Network and Parallel Computing Workshops, 2007. NPC Workshops. 2007.

[7] Naldurg, P., Campbell, R.H. Dynamic Access Control: Preserving Safety and Trust in Network Defense Operations. in Proceedings of the Eighth ACM Symposium in Access Control Models and Technologies (ACM SACMAT 2003). 2003.

[8] Chen, K.-C. et al. Cognitive radio network architecture: part II -- trusted network layer structure, in Conference On Ubiquitous Information Management And Communication 2008, ACM: Suwon, Korea p. 120-124.

[9] Clancy, T.C., Geoergen, N. Security in Cognitive Radio Networks: Threats and Mitigation in Cognitive Radio Oriented Wireless Networks and Communications, 2008. . 2008. p. 1-8.

[10] Chen, R. et al. Toward secure distributed spectrum sensing in cognitive radio networks, in IEEE Communications Magazine Special Issue on Cognitive Radio Communications. 2008. p. 50-55.

[11] Akyildiz, I. F. et al. NeXt generation/dynamic spectrum access/cognitive radio wireless networks : A survey. Computer Networks, 2006. 50: p. 2127-2159.

[12] Kondareddy, Y.R , Andrews, N., Agrawal, P. On the Capacity of Secondary Users in a Cognitive Radio Network, in Proceedings of IEEE Sarnoff Symposium 2009, New Jersey, USA, 1–5 (March 2009.

[13] Theinn, T., Park, J.S., Chi, S.D. Increasing Availability and Survivability of Cluster Head in WSN, ACM Conference 2008.

[14] Parvin, S. et al. Towards Trust Establishment for Spectrum Selection in Cognitive Radio Networks , In the proceedings of 24th AINA conference, IEEE, Perth, Australia, 2010.

[15] Akyildiz, I.F., et al. A Survey on Spectrum Management in Cognitive Radio Networks, in IEEE Communications Magazine. 2008.